POLÍTICA DE PROTECCIÓN DE INFORMACIÓN Y

PRIVACIDAD TECNOLÓGICA

A. Introducción:

Esta política muestra la importancia de proteger la información generada en la institución por sus empleados.

B. Alcance:

Que la información generada en la institución esté lo suficientemente protegida contra ataques externos y de cualquier otra índole.

C. Descripción:

La información generada en nuestra institución puede incluir en algunos casos contenidos de carácter confidencial y que requieren protección contra robo de identidad o de otra índole. Todo el contenido generado debe tener un proceso de protección de data para asegurar la información de las áreas implicadas de la institución.

D. Objetivos:

1. Asegurar la información generada por las áreas implicadas de la institución.
2. Mantener la información de la institución archivada digitalmente de forma redundante.
3. Revisar que los usuarios tengan sus propiedades de forma correcta según su rol de trabajo.
4. Orientar al personal sobre el manejo eficiente y confidencial de los sistemas de información del estudiante.
5. Realizar auditoría de sistemas de información del estudiante.
6. Realizar mantenimientos a los sistemas de información periódicamente.
7. Asegurar la confidencialidad de los records e información financiera de los estudiantes correspondientes en Asistencia Económica.
8. Controlar las pantallas de acceso a los sistemas que permiten visualizar o extraer información de estudiantes y empleados.

E. Responsabilidades:

1. El **Técnico de Computadoras,** contratado por servicios prestados, trabaja la parte del almacenamiento seguro de la información generada por los empleados de forma interna y digital (en la nube de forma automática). Se asegurará de lo siguiente:
    a. Firewall (contra piratería u otros).

b. Combatir los virus
c. Evitar ataques externos que pongan en riesgo la información generada en la institución. (Hackers y/o Crackers).
d. Proteger la información de las áreas vitales de la institución; Registraduría Tesorería y Asistencia Económica.
e. Mantener almacenada redundantemente la información generada digitalmente por los empleados.
f. La red posea la seguridad pertinente para asegurar la confidencialidad de los records financieros de los estudiantes relacionados a Asistencia Económica o áreas relacionadas.

2. **El Consultor Externo del Sistema SISAS se asegura de:**
    a. El Consultor externo del sistema SISAS asegura que cada estudiante y empleado tengan una pantalla de acceso el cual le requiera una autentificación de entrada, con el propósito de controlar los accesos a información que solamente puede ser visualizada por usuarios autorizados.
    b. La base de datos posea la seguridad pertinente para asegurar la confidencialidad de los records financieros de los estudiantes relacionados a Asistencia Económica o áreas relacionadas.

3. El personal designado de Antilles provee los accesos de cada usuario que tenga paso a la información del estudiante y que tengan el rol pertinente, de acuerdo a su función de trabajo.

F. Procedimiento:

1. El **Técnico de Computadoras**:
    a. Trabaja el almacenamiento de la información generada por los empleados y esté resguardándose internamente y en la nube de forma óptima.
    b. Observar que el firewall esté funcionando adecuadamente y continuamente.
    c. Observar que el antivirus para protección de documentos y ataques esté actualizado y activado constantemente.
    d. Revisar que el antivirus de los servidores esté actualizado y activo.
    e. Asegurar que los “routers” de la red tengan activa la protección.
    f. Mantener que la información de los estudiantes esté asegurada.
    g. Revisar que la base de datos esté resguardándose adecuadamente en tiempo real.
    h. Asegurar que la información de servidores de Antilles College of Health esté segura y resguardada.

2. El **Consultor del Sistema SISAS** se asegura de:
    a. Mantener la seguridad de autentificación de usuarios para evitar modificaciones mal intencionadas en la base de datos.
    b. Asegurar el control de accesos a información de estudiantes y empleados por medio de autentificación, esto permitirá acceder a la información a usuarios solamente autorizados.

3. El Especialista de Educación a Distancia y Tecnología Educativa debe:
    a. Revisar que los roles de cada usuario sean los pertinentes y justos para sus funciones de trabajo.
    b. Asegurarse de que cada usuario esté orientado sobre el manejo y los accesos que se le han asignado relacionados con la información del estudiante. Además de orientarles sobre la protección y privacidad de la información del estudiante.

PROCESO DE ORIENTACIÓN SOBRE CONTRASEÑAS

(CYBERSECURITY)

Empleados:

Antilles College of Health orienta a sus empleados y facultativos en relación al "Cybersecurity" (Contraseñas y cuidado de la Información) en el proceso de orientación.

Los empleados y facultativos pasan por un proceso de orientación en el cual se les adiestra y capacita en las diferentes áreas institucionales. La Oficina de Soporte Técnico, a cargo del Especialista de Educación a Distancia y Tecnología Educativa, quien orienta sobre los distintos Sistemas Informáticos de Antilles y explica el mecanismo correcto para utilizarlos. Dicha oficina asigna datos de acceso los cuales requieren un patrón de caracteres para protección.

Los empleados y facultativos son orientados mediante un documento oficial conocido **"Política de Contraseñas"** en el cual se le explica sobre la importancia de mantener una contraseña con un patrón de caracteres correcto para salvaguardar la información de la institución. Este adiestramiento busca que los usuarios sean debidamente orientados para que cuiden o protejan correctamente la información.

Se les explica que la cuenta de acceso expira frecuentemente con motivos de que cambie la contraseña actual. De igual manera se les instala una aplicación para Autentificar la identidad de la persona (MFA). Esta aplicación les permitirá aceptar o denegar acceso de autentificación.

Estudiantes:

Antilles College of Health orienta a sus estudiantes en relación al "Cybersecurity" (Contraseñas y cuidado de la Información) al inicio por primera vez en la institución.

Los estudiantes son adiestrados sobre cómo autentificarse e instalan la aplicación Microsoft Authenticator, la cual valida la identidad de los estudiantes al acceder a sus plataformas educativas. Esta aplicación les permitirá aceptar o denegar acceso de autentificación.

En el proceso de orientación se les informa sobre la importancia de mantener sus datos de acceso de manera confidencial para salvaguardar la información de sus clases.

El sistema les requiere cambio de contraseña frecuentemente para todos los estudiantes, con motivos de que cambie la contraseña actual. De igual manera se les instala una aplicación para Autentificar la identidad de la persona (MFA).

POLÍTICA DE AUTENTIFICACIÓN

INTRODUCCIÓN:

Antilles College of Health garantiza un método de autentificación seguro para los estudiantes y empleados en nuestra escuela. Nuestro principal objetivo es contar con un proceso de validación de datos de acceso de los usuarios para que puedan acceder a los sistemas establecidos en la Institución. Esta política comprende la manera en que nuestros estudiantes y empleados se autentificarán en los distintos sistemas electrónicos de la Institución. A continuación, se detallarán procesos estrictamente importantes para manejo de los datos de acceso de cada personal de la institución.

RESPONSABILIDADES:

Es importante que cada estudiante y empleado conozca las responsabilidades que debe conocer sobre la política de autentificación, a continuación, se detallan las responsabilidades:

1. Cada estudiante y empleado será orientado una vez obtenga sus datos de accesos para los sistemas informáticos de la institución.
2. No es permitido en ninguna circunstancia divulgar los datos de acceso a terceras personas.
3. Se debe mantener en completa confidencialidad los datos de acceso brindados por la institución.
4. En caso de problemas técnicos debe comunicarse con el personal de apoyo técnico.
5. Para ofrecer servicios de apoyo técnico la institución utilizará mecanismos para validar la información de la persona solicitante de servicios.

PROCEDIMIENTO:

Para asegurar que las contraseñas estén seguras se debe tomar en cuenta lo siguiente:

1. La contraseña debe tener al menos 8 caracteres
2. Los mismos deben ser una mezcla de números, letras mayúsculas y minúsculas y caracteres especiales.
3. La contraseña no debe parecerse o ser igual a la palabra contraseña de ninguna forma. Ejemplo añadir un número o incluir letra.
4. No debe ser similar al "user id" o su nombre.

5. No preste o divulgue su contraseña a otras personas, incluyendo a individuos que pretendan ser administradores del sistema.
6. Nunca tenga su contraseña visible de forma escrita
7. Nunca deje su computadora desatendida, de necesitar hacerlo cerrando la sesión.

La contraseña para acceder a los sistemas será temporal y se podrá cambiar en cualquier momento, además, los mismos sistemas requerirán cambios de contraseña en momentos predeterminados.

Los servicios de soporte técnico se ofrecerán en el Centro de Recursos de Aprendizaje y Educación a Distancia.

MÉTODO DE AUTENTIFICACIÓN PARA ESTUDIANTES BAJO LA MODALIDAD BLENDED

El Centro de Recursos de Aprendizaje y/o la Oficina de Educación a Distancia proporcionará a los estudiantes inscritos remotos datos de acceso para acceder a la Plataforma Educativa donde tomarán sus cursos.

La dirección URL que se utilizará para acceder a la plataforma Educativa es: https://aulavirtual.antillespr.edu/ (los estudiantes podrán acceder directamente e ingresar sus datos de acceso).

La contraseña para acceder a la plataforma será temporal y el estudiante puede cambiarla en cualquier momento, además, el mismo sistema requerirá cambios de contraseña en momentos predeterminados.

Cualquier estudiante que requiera soporte técnico en relación a los datos de acceso o la gestión de la plataforma educativa, el Centro de Recursos de Aprendizaje y la Oficina de Educación a Distancia proporcionará el servicio para que puedan llevar a cabo sus estudios de manera efectiva.

Las guías para acceder a la plataforma fueron desarrolladas tanto para el alumno como para el maestro, estas guías explican paso a paso el proceso para administrar y administrar la plataforma Moodle, permitiendo así que el alumno obtenga las habilidades para navegar el curso, enviar sus trabajos y llevar a cabo actividades educativas en la plataforma.

POLÍTICA DE PRIVACIDAD

La información generada en nuestra institución puede incluir en algunos casos contenidos de carácter confidencial y que requieren protección contra robo de identidad o de otra índole. Todo el contenido generado debe tener un proceso de protección de data para asegurar la información de las áreas implicadas de la institución.

Como Institución Educativa y en cumplimiento con los requisitos de seguridad informática, nuestros sistemas cuentan con alta seguridad contra los virus, troyanos, ataques malintencionados.

La seguridad en nuestra Institución es robusta, ya que contamos con las siguientes protecciones:

- Firewall (contra piratería u otros).
- Antivirus
- Control de ataques externos que pongan en riesgo la información generada en la institución. (Hackers y/o Crackers).

Para ACH es de suma importancia proteger la información de las áreas neurálgicas de la institución; Registraduría, Tesorería y Asistencia Económica. Nuestra infraestructura tecnológica cuenta con un sistema de resguardo adecuado para que la información esté debidamente almacenada de forma redundante.

La red posee la seguridad pertinente para asegurar la confidencialidad de los récords financieros de los estudiantes relacionados a Asistencia Económica o áreas relacionadas.

Cada empleado, facultad y estudiantado cuenta con controles de acceso a los sistemas que cada cual trabaja, es decir, la comunidad estudiantil podrá acceder a sus cursos por medio de una autentificación que les pedirá sus datos secretos para poder validar su identidad. Nuestros sistemas están desarrollados de esta manera para proteger la información de nuestros estudiantes, facultad y empleados.